**IN THE CLAIMS:**

The following is a list of all pending claims. Please amend the following claims as follows:

1. (Withdrawn) A method of detecting surveillance or attack activity over a computer communications network, comprising:

receiving a plurality of messages from a data sensor located at a network audit point, each of said messages describing an event occurring on said communications network;

classifying one or more of said events to produce one or more labeled alerts;

combing in one or more said labeled alerts to produce a combined alert; and

aggregating one or more said combined alerts to produce an aggregate alert notification.

2. (Withdrawn) The method of claim 1, further comprising filtering one or more said aggregate alert notifications by a cost-based model to produce a qualified alert.

3. (Original) A method of detecting surveillance activity over a computer communications network, comprising:

receiving a plurality of messages from a data sensor located at a network audit point, each of said messages describing an event occurring on said communications network;

processing one or more of said messages comprising one or more of the following:

clustering packets exchanged between the two addresses within a specified time period;

clustering packets exchanged between two addresses having certain flags set;

clustering packets exchanged between two addresses having similar flags set; and

clustering packets exchanged between two addresses having similar characteristics.

4. (Original) The method of claim 3, further comprising processing one or more said extrapolated network connections to produce a detected surveillance probe, said processing of one or more said extrapolated network connections to produce a detected surveillance probe comprising one or more of the following:

grouping connection session records over related source addresses;

scoring each group based on the quantity of attack destinations;

generating an alert for each group whose score is greater than an empirically-derived threshold;

identifying unusual packets;

identifying packets that have a particular arrangement of flags set;

identifying packets that have all flags set;

identifying packets that have payloads smaller than a predetermined size;

identifying packets to which there is no response;

identifying packets to which there is no response and that have a particular arrangement of flags set;

identifying detected connections with certain characteristics;

identifying detected connections with an unusually small number of packets;

identifying detected connections with fewer packets than a predetermined limit;

identifying detected connections with packets that have traveled only from the source to the destination;

identifying detected connections with packets that have traveled only from the destination to the source; and

identifying detected connections with packets whose payloads are smaller than a predetermined limit.

5. (Original) The method of claim 4, further comprising the control of false positive detections vs. false negative detections.

6. (Original) The method of claim 4, further comprising generation of a profile of surveillance activity, said profile of surveillance activity comprising one or more of the following:

a breakdown of probes;

the number of attackers;

the number of attacks per unit time;

the percentage of activity that constitutes malicious surveillance;

the breakdown of source country frequencies;

the most frequently-targeted network addresses; and

the temporal frequency trends of individual attackers.

7. (Original) The method of claim 4, further comprising processing one or more said detected surveillance probes to produce a detected surveillance scan, said processing of one or more said detected surveillance probes to produce a detected surveillance scan comprising one or more of the following:

modeling and detecting surveillance scans as a series of surveillance probes that originate from one or more source addresses and that are sent to one or more destination addresses;

modeling and detecting surveillance scans performed by a particular source address by identifying a particular source address that sends more than a specified number of probes;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that generates more than a specified number of probes within a specified time period;

modeling and surveillance detecting scans performed by one source IP address by identifying a source address that sends probes to more than a specified number of destinations;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to a specified set of destinations;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to specified ports;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to a number of destinations in excess of a specified limit within a specified time period;

limiting the number of detected scans by reporting only source addresses that perform more than a specified number of probes within a specified time; and

limiting the number of detected scans by reporting only source address groups that perform more than a specified number of probes within a specified time.

8. (Original) The method of claim 7, further comprising the control of false positive detections vs. false negative detections.

9. (Original) The method of claim 7, further comprising generation of a profile of surveillance activity, said profile of surveillance activity comprising one or more of the following:

a breakdown of probes;

a breakdown of scans;

the number of attackers;

the number of attacks per unit time;

the percentage of activity that constitutes malicious surveillance;

the breakdown of source country frequencies;

the most frequently-targeted network addresses; and

the temporal frequency trends of individual attackers.

10. (Original) The method of claim 7, further comprising processing one or more said detected surveillance scans to detect a group of scanning hosts, said processing of one or more said detected surveillance scans to detect a group of scanning hosts comprising:

modeling and detecting scans distributed across a series of source addresses by grouping addresses, said grouping of addresses being performed by subtracting one address from another and placing the two addresses in the same group if the difference is less than a specified amount.

11. (Original) The method of claim 10, further comprising the control of false positive detections vs. false negative detections.

12. (Original) The method of claim 10, further comprising generation of a profile of surveillance activity, said profile of surveillance activity comprising one or more of the following:

a breakdown of probes;

a breakdown of scans;

the number of attackers;

the number of attacks per unit time;

the percentage of activity that constitutes malicious surveillance;

the breakdown of source country frequencies;

the most frequently-targeted network addresses; and

the temporal frequency trends of individual attackers.

13. (Withdrawn) A method of detecting surveillance or attack activity over a communication network comprising:

combining alerts to such surveillance or attack activity generated by an intrusion detection system with alerts to such surveillance or attack activity generated by an anomaly detection system to produce a combined alert;

prioritizing said combined alert to produce a prioritized alert;

presenting said prioritized alert to a security analyst.

14. (Withdrawn) A computer program product for use in conjunction with a computer system to classify and analyze surveillance or attack activity over a communications network, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

an event data storage buffer that receives and stores incoming event data;

an initial event evaluator that receives event data from said event data storage buffer and generates raw alerts;

a raw alert data storage buffer that receives and stores said raw alerts;

a post-processing alert evaluator that receives said stored raw alerts and produces processed alerts;

a plurality of alert filtering modules that receive said processed alerts and produce user alerts;

a user alert data buffer that receives and stores said user alerts;

a plurality of production models for said initial event evaluator;

a plurality of production models for said alert filtering modules;

storage for said production models for said initial event evaluator and for said production models for said alert filtering modules; and

an automated job submission manager that orchestrates the operations of said initial event evaluator and of said post-processing alert evaluator.

15. (Withdrawn) A computer system for formatting, classifying and analyzing surveillance or attacks over a communications network, the computer system comprising:

a central processing unit;

a memory, coupled to the central processing unit, the memory storing:

outputs of sensors connected to the communications network;

outputs of an initial event evaluator;

outputs of a post-processing alert evaluator;

outputs of a plurality of alert filtering modules;

a plurality of production models for said initial event evaluator; and

a plurality of production modes for said alert filtering modules.

16. (Withdrawn) A method of processing computer network surveillance alerts, comprising:

receiving alerts from an intrusion detection system;

receiving alerts from an anomaly detection system;

receiving alerts from a scan/probe detection system;

aggregating one or more of said alerts from said intrusion detection system , said anomaly detection system, and said scan/probe detection system; and

generating an aggregated alert.

17. (Withdrawn) A user display for profiling surveillance activity over a computer network, said user display comprising: a display of a numerical estimate of the severity of an attack and one or more of the following:

a list of the highest priority threats;

a list of the highest priority targets;

detailed threat information;

detailed target information;

the country of origin of an attack;

the country of origin of a target; and

a plot of attack severity versus time.

18. (Withdrawn) A method of detecting surveillance or attack activity over a computer communications network, comprising:

modeling network connections;

detecting said network connections that are likely surveillance probes originating from malicious sources;

detecting scanning activity by grouping source addresses that are logically close to one another; and

recognizing certain combinations of said likely surveillance probes.